SFA Modernization Partner

United States Department of Education

Student Financial Assistance

Integrated Technical Architecture

Detailed Design Document

Volume 5 – Security Architecture

Task Order #16

Deliverable # 16.1.2

October 13, 2000

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1. Purpose

The Security Architecture (SA) volume within the Integrated Technical Architecture (ITA) Detailed Design Document (DDD) will provide an overview of the security requirements, gaps between the current environment and the requirements, and architectural recommendations for the Release 1 of the ITA. Applications that will leverage this release of the ITA include: Schools Portal, Information for Financial Aid Professionals (IFAP), and Intranet Release 2.0.

1.2. Scope

This document covers Student Financial Assistance (SFA) Security Architecture and includes:

- Security Framework Overview
- Analysis of the Current Environment: An assessment of SFA's current security framework for the Release 1 applications (IFAP, School Portals, and Intranet Release 2.0) as well as future releases of SFA applications.
- Proposed Architectural Designs: A proposed security framework based upon Common Operating Environment (COE) and Internet Security Standards Task Order 4 Deliverable 4.1.3.
- Gap Analysis of Current Infrastructure: An analysis of the security needs required to fulfill the proposed architectural design both short and long term.
- Architectural tool recommendations, options, and implementation examples.

1.3. Approach

The following approach was used to develop the SFA Integrated Technical Architecture Security Architecture. The SFA documentation of existing and future SFA systems was reviewed.

Systems that were evaluated for the Gap Analysis for Release 1 include:

- IFAP
- Schools Portal
- Intranet Release 2.0

Systems that were evaluated for the post -Release 1 included:

- Campus Based Systems (CBS)
- Central Processing System (CPS)
- Direct Loan Consolidation System (DLCS)

- Direct Loan Origination System (DLOS)
- Direct Loan Servicing System (DLSS)
- Federal Family Education Loan (FFEL)
- Multiple Data Entry (MDE)
- National Student Loan Data System (NSLDS)
- Post-secondary Education Participants System (PEPS)
- Recipient and Financial Management System (RFMS)
- Title IV Wide Area Network (TIVWAN)

After reviewing the pertinent documents, meetings were held with members of the SFA Chief Information Office (CIO) executive team, channel owners, Virtual Data Center (VDC) support personnel, and various hardware/software vendors who provide services and support for SFA.

From the information gathered from these resources as well as internal knowledge capital, the SFA Security Framework document was completed. This document describes the architectural requirements, gaps, and components of the SFA Security Framework, which addresses several security paradigms: fine-grained access control, authorization, authentication and single sign-on potential. The combination of these functions within a single entity, conceptually referred to as an enterprise security portal, will provide SFA with a secure, reliable, and available framework to its varied applications, Web sites, and databases.

1.4. Audience

This security architecture document is aimed at an audience of technical architects, designers and developers charged with creating network-based solutions. This document assumes that the reader is knowledgeable in security and network-based solutions.

1.5. Security Assessment and Gap Analysis Summary

Currently, the Department of Education (DOE) Student Financial Services (SFA) systems are maintained within an adequate security architecture design for the perimeter level protection of applications housed within their data centers. Appendix A is a matrix, which depicts specific, case by case analysis of current products purchased and implemented.

A summary of findings is provided below:

- **Network Perimeter Security –** The network perimeter is designed for protection via multiple layers of network security. Cisco routers are utilized across the environment, packet-sniffing software is installed to protect against denial of service attacks, and both inbound and outbound network traffic must pass through a Checkpoint firewall. The products used by SFA for perimeter protection are all very respected within the industry and rank at or near the top of their class according to industry statistics and think tank groups such as Gartner and Giga. These solutions have the capability to resolve the

majority of the network security issues with proper configuration. A detailed analysis of router and firewall configuration is necessary before determining if adequate measures are completely in place for comprehensive perimeter security.

- **Significant Comments –** At the time of this assessment**,** implementation of scheduled network vulnerability assessments and the formation of a Computer Emergency Response Team (CERT) is in progress. Execution of these functions is necessary to regularly monitor the SFA environment for the existing presence or new introduction of vulnerabilities, network exposure, or potential exploits as well as enabling SFA with a procedure to react and respond to system or network emergencies. Furthermore, these functions are key to solid risk analysis and business resumption capabilities.
- **Information Security Standards of Configuration –** A set of written documents is needed outlining policies and procedures for the configuration of all SFA Information Systems to ensure minimal security exposure. These standards of configuration are needed at varying levels, from general standards to operating system specific standards to application-level standards. The establishment and implementation of such standards enables the SFA to measure the level of security compliance within the organization. Such standards should be applied to all information systems connected to SFA networks regardless of ownership. In addition, establishment of minimum standards, in correlation with policy compliance assessment tools, drastically reduces lost resource time necessary for conducting system audits.
- **Host-Based System Protection –** Tripwire is currently used in a limited capacity for file access monitoring. Tripwire is a specialized product with the purpose of monitoring access to designated critical files. However, more comprehensive host and network-based intrusion detection systems, policy compliance assessment, centralized log collection and decision-based reaction tools are available.

  The security posture on SFA host operating systems is currently inadequately monitored. The Control SA product from BMC Software was purchased to assist with system security requirements, but this product is targeted at security management on mainframe applications. Distributed computing environments present a greater level of risk to the organization and should be monitored accordingly. Host-based intrusion detection products and policy compliance assessment tools are available and highly recommended. Such tools monitor and assess the host in accordance with the established Information Security standards of configuration.

1.6. SFA Security Framework Recommendations Summary

Current Security Assessment: The current SFA network architecture provides a satisfactory level of perimeter-level protection for the ITA systems for Release 1.

Overall Recommendation for Release 1: The Release 1 systems should continue to be enhanced from a security perspective. There are certain security features, which should be implemented as these systems proceed and these features apply to the overall SFA architecture as well.

Implementation of the following is recommended:

- Intrusion detection systems are needed at both a network and host level. Regardless of the protection provided at a firewall level, systems should be monitored for intrusion. Firewalls present a first line of defense but no single element of security provides comprehensive protection. As is the case in physical security if someone attacks and penetrates a steel door with three deadbolt locks, an alarm should alert the proper group of the compromise. This scenario applies the same to the network perimeter and internal systems housing critical applications. If the firewall experiences a compromise, an automatic alarm is triggered and a log of all activity is made available by network intrusion detection systems. Specific Vendor Product Recommendations are provided in Appendix A (Rows 1-4).
- Policy compliance assessment tools are recommended. These automated tools provide security configuration compliance baselines and measure for deviations from that baseline at scheduled intervals. Reports provide system administrators with detailed recommendations needed to resolve problems found. Vendor Recommendation provided in Appendix A (Rows 5-6) under the Information Security Core Technology Status section.
- It is highly suggested that all systems scheduled for Release 1 have a thorough vulnerability assessment conducted after code freeze, but prior to production rollout. Currently, it appears that the Modernization Partner and CSC are planning to conduct these tests. Tests should include analysis of application code as well as host systems and networks. Vendor recommendation provided in Appendix A (Row 3).

Overall Recommendation – Post- Release 1: SFA should continue to build active defenses from intrusion for all systems, starting with the systems being delivered for Release 1.

In addition to the recommendations for the Release 1 applications, the following tasks should be accomplished post-Release 1:

- A centralized monitoring, log-collection and reporting solution to support real-time intrusion detection and overall security management is needed for the SFA Security Infrastructure. Automated tools exist which can collate information from a variety of sources (firewalls, intrusion detection devices, policy compliance tools, etc), facilitate alert mechanisms, and provide summary reporting. This alleviates the extensive man-hours required to sift through log files, which ultimately delay detection of network penetration until well after the fact. Such a system supports near real-time reporting, versus post incident reporting. Vendor Recommendations provided in Appendix A (Rows 2, 3, 8-11).
- An Information Security standard of configuration is required for each major technology component (e.g., Sybase, Oracle, NT, Solaris, IIS, etc). These baselines provide product specific details to developers and architects to for secure configuration of SFA systems and allow establishment of technical security parameters on each system. The result is a more common system level build, testing structure, configuration management structure, and stronger overall data integrity. Vendor Recommendations provided in Appendix A (Row 10).
- An enabling Security Framework architecture will allow SFA to move away from the current "hairball" development methodologies. Such architecture will provide an

infrastructure supporting Information Security initiatives during the application development cycle and consists of several minimum components to include:

- Lightweight Directory Access Protocol (LDAP)
- Privacy Management
- Central Risk Management
- UserID Management
- Application Programming Interface (API)/Toolkits for SFA integration to MQ, WebSphere, Java, and Common Object Request Broker Architecture (CORBA)

and also support a Portal based architecture. Vendor Recommendations provided in Appendix A (Row 15).

- It is recommended that SFA implement a formal Risk Assessment program. The purposes of this program is to:
  - Provide business managers with a process to integrate security risk management into the decision support process for business operations.
  - Implement a business-risk based approach to identifying and assessing information security risks in the terms of the impact on business operations.
  - Provide the business manager a basis for determining what controls are needed and what level of resources can be expended on controls.
  - Appendix B, System Technology Risk Matrix provides a technology risk matrix, as a starting point for this process.

2 Security Framework Overview

The SFA program is moving to allow its customers and its partners high-speed, secure system access over the Internet. In order to make this happen, the architecture that supports this access must provide confidentiality, identification, authentication, authorization, data integrity, accountability, and non-repudiation for all transactions initiated.

The Security Framework is a usable and comprehensive security overview. This Security Framework should be thought of as a conceptual structure used to frame the security related work to be designed and implemented.

This Security Framework is used to help SFA understand what security components may be required and how the components fit together. Based on the inventory of components and the description of their relationships, the optimal solutions will be applied.

Multiple instances of security frameworks may be necessary to facilitate business needs. The number and location of these infrastructures will be driven by business and institutional needs enabled by security, performance, and quick reaction capability. If more than a single framework is required, the directory structures for each framework can be replicated across the infrastructures. In the case of an infrastructure failure, traffic can be routed to another framework providing redundancy of operations transparent to the end-user. Each framework can be configured for high availability sharing processing loads across infrastructures. Where multiple infrastructures are implemented to provide a common set of security services, the virtual aspect of framework design can be used to balance the load across diversely located SFA systems thereby achieving optimal utilization of SFA resources and reducing capital investment.

The components of an Enterprise Security Framework will consist of:

- Business Assets - represents what needs protection, and is the target of all information security efforts. The SFA Security Framework will contain all the necessary hardware and software to secure most SFA resources including legacy applications (client server and mainframe). The framework should furnish the necessary features that make the secure implementation of Business-to-Customer, Business-to-Business, and internal based systems more efficient and systematic.
- Risk Management - analyzes the value of business assets, the cost to protect the assets, the level of protection required, and discovers the threats and vulnerabilities that must be addressed through the security strategy. The Security Framework provides event monitoring, logging and detection of multiple types of activities. Implementation of the Security Framework allows detection when an event occurs that violates the system's security policy, generates alerts, and allows administrators to determine how to respond to the attempt.
- Security Strategy - defines the approach and direction SFA is taking to secure and enable the Business Assets in line with the Risk Management approach. Within industry and government most major systems development, communications, and financial

transactions are moving to an Internet. No longer is it enough to provide basic security commodity services (firewalls, secure routers, virus protection, etc) which block and disable, but it is also crucial to be able to provide enabling services to allow all financial institutions, academic organizations, and individual users to securely access SFA resources over the Internet. The focus of this document is to provide analysis of the current services employed at SFA, verify security at network perimeters, and provide emphasis on enabling technologies and solutions which support security within the SFA business model.

- Security Policy and Standards of Configuration - aims at achieving a secure environment by establishing consistency in architecture and to reducing the risk, effect and cost of security incidents. The SFA Security Framework will furnish centralized control to maintain SFA security policy. It will deliver the flexibility to control and manage access through the Security Framework from a central location. These features include an easy to use management interface, configuration of remote sites and monitoring of all systems from a centralized location. Access control rules will be established in accordance with SFA security policy. The SFA Security Framework will provide sophisticated access controls defined through measures such as time, day, user groups, network groups, network interface, inbound & outbound authentication, and encrypted tunnels.
- Security Management / Operations – covers the overall responsibility for the management of the secure enterprise as well as monitoring of the security infrastructure. Within this section, roles and responsibilities will be identified. Central onsite and remote management capability is necessary to accomplish the network administration concerns of SFA. The configuration of remote sites from a centralized location provides an additional layer of administration and control of information security. This is accomplished through use of strong authentication mechanisms and Virtual Private Network (VPN) technology. Analogous to the need for remote administration, the delegated administration of users is essential for efficient systems management. Management of users inside and outside SFA should be delegated to an infrastructure at the lowest common denominator, such as an academic financial administration group.
- Security Awareness – communicates the security policies and procedures to all employees, business partners and customers to set expectations regarding information security. Awareness programs establish and communicate individual responsibility for protecting the confidentiality, integrity and availability of business assets. The awareness program is used to communicate Information Security policies and standards of configuration to all personnel responsible for handling, administration, or maintenance of systems containing SFA related electronic information.
- Security Compliance - includes all functions necessary to ensure that the security policy and standards of configuration are created, implemented, measured, enforced and updated as required. The SFA Security Framework enables two levels of security compliance. It will monitor the SFA infrastructure for intrusion detection and policy compliance, while the combination of routers and firewalls will verify the authenticity and integrity of Internet users that are attempting contact. The SFA Security Framework will provide fine-grained proxy services that will authenticate, authorize, and control access to limit activity between the two internal and external network interfaces, thus, disallowing any direct communication between the two network interfaces. .

- Security Administration - performs administrative processes, primarily oriented towards managing users of SFA system resources. The SFA Security Framework will have a management interface to allow efficient administration of access rules policy management. Security administrators can set security parameters, control access, and monitor activity through this interface. Access rules allow control of connections based on time, date, user groups, network groups, network interface, inbound & outbound authentication, and encrypted tunnels.

  To create a secure domain, all functions provided by the SFA Security Framework must be administered via a common interface. This administrative interface will specify how the requesting user (no matter where located) will be allowed to participate in SFA secure domain. The SFA Security Framework will broker all the underlying network issues and security precautions to make the SFA Extranet, Intranet and Internet secure.

- Security Services for Application Development - supports and enables the development of new security technologies, applications, systems, and business capabilities, with the ability to tie into the Security Framework. The architecture will support Application Security, Authorization, and integration with Websphere, Applets, Servlets, Enterprise Java Bean (EJB) components, CORBA, Java, and Legacy applications via standards and customizable APIs.

  Several categories have been identified for which adequate interfaces would need to be defined. The identified categories are:

  - Registration and Initialization (as necessary)
    - The process of establishing an identity on the resource
  - Authentication
    - The process of proving your identity
  - Credential Management
    - Managing the security identity attributes after authentication
  - Simple Authorization
    - Process of determining the rights of a user on a specific resource
  - Entitlements
    - Abilities granted to application user
  - Quality of Protection (QOP)
    - The level of information security
  - Delegated Authorization Administration
    - Ability of the framework to allow decentralized management of credentials and entitlements
  - Auditing
  - Interceptors
    - Framework service allowing applications to utilize security components and databases without custom programming, thus making security implementation almost transparent to developers

- Web Proxy / Portals
  - Intermediary between application and the Internet
- CORBA Interceptors
  - Interceptor designed for CORBA based applications
- MQ Exits
- API Wrapper (used where Interceptors are not applicable)
  - Method for application programmers to write calls to services of the security framework
- Single API for authentication (easy migration: userid / password → SecurId → Certificates)
- Few Authorization APIs
- Few APIs for encryption, digital signature (without developers worrying about what algorithms to use)
- Single API for event monitoring, logging, and alerting
- Common Administration Framework
- Improve operations efficiency by developing customized admin consoles (that can synchronize information across security registries.)
- The Security Framework will develop a standard Process to engage with Developers (Reduce overall engagement time frames of work per application)
- Collect key information from developers
- Ask application architect to provide a (standard format) technical architecture diagram
- Determine the level of security required
- Produce a security integration document
- Actual development & Testing

- Security Services for Network Architecture– supports re-useable common network security architecture components that have been documented and packaged to facilitate easy re-deployment. The SFA Security Framework will offer security for the SFA Infrastructure. It will offer a full security for all TCP / IP and legacy applications, presenting an implementation of a transparent gateway.

  The SFA Security Framework should include:

  - Full authentication, authorization, and access control for all traffic (Extranet, Intranet and Internet).
  - VPN access for remote users (replacement / augmentation for dial-in).
  - VPN access for extranet partners, vendors, service providers, and relationship based business associates.
  - Traffic statistics, logging, intrusion detection, and real-time alerting
  - Network address translation services.

- Two factor authentication services.
- Delegated administration of users.
- Definable data filtering
- Centralized management interface.

- Security Infrastructure – consists of the hardware and software components that provide protection for the Business Assets. The SFA Security Framework will contain all the underlying services responsible for ensuring a secure environment for Extranet, Internet and Intranet access, including single sign-on. Network and security mechanisms will include interaction with routers, firewalls, and any necessary encryption functions.

  A single SFA Security Framework requires global directory and registry function that will contain lists all the valid users, groups, organizations, and password information necessary to provide inclusive single sign-on functions. The directory structure will contain an account entry for all valid security entities within a SFA domain. The SFA Security Framework should work directly in conjunction with existing directory services such Exchange servers supporting corporate email and DB2 systems supporting current user populations within the legacy systems. The SFA Security Framework will allow for extensibility of services, to include integration with current network load balances, Virtual Private Networks and token authenticators as well as future initiatives such as the GSA-ASIS Public Key Infrastructure (PKI) project and Smartcard projects

  Note: For more information on the Security Framework components and their relationships refer to the "Security Framework" document included in Task Order 4 Deliverable 4.1.3.

3 Analysis of Current Environment

3.1. Business Assets

An analysis of the current environment allows SFA to understand at a detailed level the "as is" state of SFA legacy security systems. The information provided in this document represents a starting point for understanding the current technical security environment, and will be used to facilitate a migration strategy for integration with the Integrated Technical Architecture security plans and gap analysis. This sections references the information provided in Deliverable 16.1.1 Legacy Inventory Report, interviews with current SFA employees, analysts and contractors, and evaluation of various documents developed by a variety of sources within Department of Education.

Systems that were evaluated for the ITA Release 1 included:

- IFAP
- Schools Portal
- Intranet Release 2.0

Systems that were evaluated for the post-Release 1 included:

- Campus Based Systems (CBS)
- Central Processing System (CPS)
- Direct Loan Consolidation System (DLCS)
- Direct Loan Origination System (DLOS)
- Direct Loan Servicing System (DLSS)
- Federal Family Education Loan (FFEL)
- Information for Financial Aid Professionals (IFAP)
- Multiple Data Entry (MDE)
- National Student Loan Data System (NSLDS)
- Post-secondary Education Participants System (PEPS)
- Recipient and Financial Management System (RFMS)
- Title IV Wide Area Network (TIVWAN)

Processes should exist to allow an ongoing assessment of the state of security within the current environment. Procedures should be implemented to conduct such analysis at a periodic interval not to exceed once annually.

3.2. Risk Management

The underlying *risk* of performing financial and confidential transactions on the Internet is loss of business. This can come as a result of malicious or fraudulent activities, which results

in lost credibility due to a public reputation of having an insecure means of conducting transactions. In order to protect from malicious and fraudulent activity and maintain credibility, controls must be provided for availability, integrity, and confidentiality.

Risk Management must be conducted as a business process to identify and prioritize information resources. By doing so, focus can be targeted at mission critical systems and application. This allows Information Security to prioritize security level requirements and incident response procedures based on an assigned degree of risk.

At the time of this assessment no formal Risk Management process exists. Limited solutions are in place for purposes of risk reduction, such as firewall log monitoring and use of the Tripwire monitoring tool. However, Risk Management is a comprehensive process, which requires procedures for inventory, prioritization, assessment, monitoring, and reporting. A formal Business Risk Assessment process is needed for comprehensive analysis of all current information resources and technology processes as well as the procedures for conducting pre-release analysis of all new systems and applications. Priority should be given to the implementation of risk management processes surrounding the network perimeter and host-level security.

3.2.1. Network Perimeter Security

The current network perimeter is designed in a layered architecture with the intent of forming multiple layers of control. Routers, firewalls and packet-sniffing software are currently installed to protect the network perimeter. A detailed review of access control lists as well as firewall rule sets should be conducted by an outside party.

Vulnerability assessments and penetration tests should be conducted at the network perimeter by a trusted third-party. Currently, the Modernization Partner, in conjunction with CSC, is planning to conduct such tests. A high degree of priority should be given to these tasks to ensure completion prior to release of the ITA.

3.2.2. Host Server Level Security

The security posture on SFA host operating systems is currently inadequately monitored. BMC's Control SA product was purchased to assist with system security requirements, but this product is targeted at security management on mainframe applications. Distributed computing environments present a greater level of risk to the organization and should be monitored accordingly. Host-based intrusion detection products and policy compliance assessment tools are available and highly recommended. Such tools monitor and assess the host in accordance with the established Information Security standards of configuration.

Tripwire is currently used in a limited capacity for file access monitoring. Tripwire is a specialized product with the purpose of monitoring access to designated critical files. However, more comprehensive host and network-based intrusion detection systems, policy compliance assessment, centralized log collection and decision-based reaction tools are available.

3.3. Security Strategy

SFA and Data Center Management have followed a sound approach in terms of defensive security measures. This includes router level security, firewall configuration, virus protection, denial-of-Service protection and human protective issues such as background checks. In areas of known deficiency (Policy development, security architecture, and penetration studies), SFA has engaged resources to assist in problem resolution.

SFA management has correctly identified need for focus on improvement of security technologies to support the business functions and Internet security paradigms. However, these areas require further exploration, product purchase and implementation into SFA environments to fully support systems such as Schools Portals, Intranet Release 2.0 and IFAP.

3.4. Security Management

SFA management has identified issues pertaining to Information Security, delegated resources to these issues, and began organizational evolution towards a single, centrally-managed security infrastructure.

The current analysis, design, and implementation of security functions should continue as planned. Maturity of a single, centrally-managed security infrastructure within large organizations is a long-term process and can take several years.

Robust defensive security measures (Priority 1) to protect SFA systems for business continuity have been implemented and are maturing with the assistance of the Modernization Partner and Computer Sciences Corporation (CSC).

SFA should begin to focus on the enabling security technologies (Priority 2), which will support the business model functions and Internet Portal architecture for SFA applications. Continued emphasis will be required to enable security technologies in support of SFA's business functions and Internet Security paradigms.

3.5. Security Policy and Standards

The Department of Education and the Modernization Partner have successfully completed the business portions of Security Policy, Standards, and Security Manager Training and Education documentation. However, current policies and standards do not include technology-specific standards of configuration for areas such as operating systems, database platforms, web server configuration, router configuration, and messaging system configuration. These specific standards must be complete to ensure the security policies are enacted across all SFA technology.

3.6. Security Awareness

SFA and the Modernization Partner have completed a series of documents targeted at Information Security Policy and Standards. Distribution of these documents is a beginning to employee awareness of Information Security efforts. Application developers, business

analysts, and management demonstrate knowing the importance of protecting organizational information and the implications involved when moving applications to the Internet.

In addition, he Department of Education website documents and references security and privacy controls to its users and customers. Legal warnings are posted within the website to discourage violators and inform users of legal restrictions which could result in prosecution.

However, a formal security awareness effort should be implemented with the mission of informing employees, users, developers, partners and vendors of the SFA Information Security strategy and policy. A formal training program is needed to ensure individuals are aware of security, privacy, fraud, and audit requirements. Such a program can be instituted in conjunction with employee orientations and should at minimum require the employees to sign an acknowledgement of awareness as well as a non-disclosure / confidentiality agreement.

3.7. Security Compliance

The SFA Security Framework should allow management to understand their current security posture in terms of compliance with an established standard of configuration for the given technology. SFA currently does not have documented stands of configuration nor do they possess the necessary monitoring tools to assess such posture. Although external access to network is restricted by routers and firewalls, it is necessary to ensure a minimum level of security at the system level in order to provide comprehensive security in the case of unauthorized network access.

3.8. Security Administration

SFA Security Administration is complex due to the multitude of business partners, customers, universities, and legal restrictions involved. Due to this vast complexity of business functions, a complete assessment of security administration procedures should be conducted to understand the current health of the process. From a high-level analysis, the UserID administrators are currently performing their duties in accordance with existing procedures.

Currently, access information is often hard-coded into business logic to define access to a certain system (e.g., Pell). Individual users request access through the Data Center. The Data Center approves access and individual or organizational access is granted. However, this access mechanism is implemented on a system by system basis with no common framework for access or automated user self-help mechanisms in place for this such as automatic password resets, lost passwords, or disablement of old passwords.

The current administration processes, although moderately secure results in heavy manual intervention, delays in system level access, and difficulties in managing users. Implementation of centralized policy and user administration will improve process flows as well as utilizing sound UserID delegation to delegate much of the data entry tasks to the

financial institution, partner, or user level. Approval and oversight would be maintained centrally, while data capture of user information could be delegated local.

3.9. Security Operations

CSC provides Security Operations support. Documentation regarding the operational aspects of security was not provided as part of this assessment. However, as a result of interviews, discussions with technical staff, and reviews of documents, it is concluded that Security Operations actively employs all security tools, methods, and technology made available by CSC. Additional documentation is required to provide a full analysis of the Security Operations function.

3.10. Security Services

Security Services supports re-useable common security architecture components. Within the VDC, the majority of the security tools and products purchased (e.g., Firewalls, routers, Virus detection) are executed in a standard re-useable fashion. The bulk of these services are for defensive security.

The Security Services offered currently lack a consistent Security Framework to enable applications, Internet Portals, and web content. Each implementation instance or system accomplishes application and web content security in a different fashion. A common Security Framework will speed application developer timelines, improve efficiency of security, and offer customers further ease of use in terms of personal UserID maintenance.

3.11. Security Infrastructure

The attached Information Security Core Technology Status provides full details of the current security infrastructure. CSC manages the network infrastructure and current security-related, architectural components (firewalls, routers, virus protection, etc) provide an adequate design for perimeter security. Hardware and software purchased by the CIO's administration is being implemented and executed within expectations. As gaps, architectures and recommended tools are defined, it is reasonable to assume that CSC will act upon the tools and implement as time / resources permit.

4 Proposed Architectural Designs

4.1. Business Assets

This section quantifies the Information Security Architecture to support the current and future SFA environments.

- IFAP
- Schools Portal
- Intranet Release 2.0

Systems that were evaluated for the post October release included:

- Campus Based Systems (CBS)
- Central Processing System (CPS)
- Direct Loan Consolidation System (DLCS)
- Direct Loan Origination System (DLOS)
- Direct Loan Servicing System (DLSS)
- Federal Family Education Loan (FFEL)
- Multiple Data Entry (MDE)
- National Student Loan Data System (NSLDS)
- Post-secondary Education Participants System (PEPS)
- Recipient and Financial Management System (RFMS)
- Title IV Wide Area Network (TIVWAN)

4.2. Risk Management

The underlying *risk* of performing financial and confidential transactions on the Internet is loss of business resulting in loss of revenue. This can come as a result of fraudulent data manipulation or as a result of lost credibility due to publicity related to having an insecure means of conducting transactions. In order to avoid unauthorized access and maintain credibility, controls must be provided for availability, integrity, and confidentiality.

The following table is an example of Risk Matrix. The table identifies system risks and threats, controls to mitigate those risks and threats, and the residual risk. A Risk Matrix should be completed for business process and the technology used within the process (Reference Appendix B). All potential internal (i.e. partners, employees) and external (i.e. customer, attacker) threats should be considered.

The table is pre-filled with some examples. The “ref. #” column refers to labeled points in application and network diagrams which show locations where compromises can occur and are specific to the application.

Table 1 - Example System Risks and Threats Matrix

Risk	Layer	Type of Compromise	Ref #	Control	Residual Risk
Denial of Service	A	Account Lockout		Self-select UID and PW – min length 7, require alpha and numeric, 3x lockout for 24 hours	Low
				Application-level security event logging	
	N	Flood Network		RTID Devices	Low
				Firewalls	
	N	Bring down network devices		SecurID	Low
				Regular password changes	
	N	Bring down operating system		ESM	Low
				ITA	
Unauthorized User	A	UID and password guessed		Self-select UID and PW – min length 7, require alpha and numeric, 3x lockout for 24 hours	Low
				Dictionary check	
	A	If someone can modify the browser, they can get access to the following: • Their own primary encrypted password • Their own remote service ID password		None	None

Legend: A – Application ; D – Data ; N – Network ; O – Operating System ; P - Physical

(The table is intended as an example and may not be comprehensive)

4.3. Security Strategy

SFA should continue to improve security mechanisms already in place such as firewalls, router configurations, anti-virus solutions, and database security. These functions and features are already purchased and the VDC is executing security aggressively for products already purchased.

SFA should then purchase the necessary hardware and software to create robust intrusion detection, real-time alerting, policy compliance, and centralized reporting capabilities. These recommendations are covered in the Gap Analysis portion of this document.

SFA's primary focus should then shift toward enabling the security services expanded upon within this document. The majority of these services revolve around the ability to move all user data into a comprehensive directory (LDAP) from existing systems such as (NSLDS) so applications can share a common repository of user data and credentials. Next, SFA should apply fine-grained access controls and authorization controls over a variety of user spaces for customers, partners, suppliers, and employees.

Course grained access control systems such as firewalls do not provide the necessary security to control access, authorization, and authentication. The following paragraphs contain a functional description of a centralized security architecture. The functions described herein are the criteria that a system of this type should exhibit.

A centralized security architecture provides a suite of modules that furnish security, management, and high availability services based on user, category of user, or group rather than Uniform Resource Locator (URL).

A management interface is utilized to establish the user or group policy. An access management subsystem has the capability to obtain and cache policy information. This information is used to enforce access policies on web applications. Authentication is verified via the access management interface to user request acceptance processing.

If user identification and authorization via public-key X.509 V3 certificate credentials is desired, this architecture supports Public-Key-Infrastructure (PKI) integration. This architecture is independent and can be configured to integrate multiple PKIs (e.g PGP, Entrust and Verisign) for authentication. It also supports simultaneous operation utilizing both username / password and X.509 / PKI based authentication.

If user identification and authentication is desired via third-party security services or application logic (e.g., cookies, SecurID, crypto tools, X.509 certificates, etc) the architecture will accommodate the request. The architecture can integrate or replace multiple Certificate Authorities, Distributed Computing Environment (DCE), Kerberos or other custom-built security applications.

The Security Framework architecture maintains the Web space (or the Web object tree) by managing and securing the web objects within that space. Typical web objects include Hypertext Markup Language (HTML) pages, plain text files, directories, ActiveX Server applets, Java applets, and Perl / Common Gateway Interface (CGI) scripts. Further, the access management component will maintain all the underlying services responsible for ensuring a secure environment. It will maintain the security database or directory, which houses all valid users, groups, and organizations that comprise the secure domain. The security database or directory contains an account entry for all valid security entities within the domain. Security entities sometimes referred to as principals, include individual users and / or servers.

As an end-user moves from machine to machine, their identities follow them, so access is not limited to designated machines. Security policies should be based on business rules, not on physical network topology. The centralized security architecture enforces access policies defined for users, groups, and for roles.

Authorization should be based on user or group roles and policy should be applied to network servers, individual transactions, database requests, specific web-based information, management activities, or to user-defined objects. The service should be extensible and should be capable of calling other authorization services for additional authorization processing. Once authenticated, the user should be granted credentials, and access control decisions should be made based on those credentials.

Identification, authentication and authorization are different functions and the split should provide a flexible and extensible authorization backbone for the Enterprise.

The centralized security architecture should manage control of access to all network resources. This authorization service must provide APIs for various applications (e.g., CORBA, Java, C++, etc). It ideally should provide a distributed and scalable authorization service that can be used as a non-intrusive (i.e., no or minimal modification of existing binaries) service to control access to all web-enabled applications. It should provide the mechanism that allow in-house developed applications to call this service directly and provide end-to-end session data encryption as needed. All attempts (both authorized and denied) to access protected information should be audited and logged. The system should provide a secure interface to manage the security infrastructure. It should be used as a non-intrusive external authorization service. The system should provide a management console(s) that is easy to learn and use, and should be capable of providing centralized control over all resources managed by the system.

The system should log all attempts to access secured information, including who makes those attempts, and whether or not the attempt was successful. This allows the system generate a complete audit trail. The auditing service ideally should be capable of being integrated with a third-party database system to perform sophisticated data analysis such as identifying hot spots or monitoring the usage of individuals. This will require the implementation of time services on networks and systems.

The system should provide authorization policies that can be defined and deployed using a centralized management console that enables administrators to define network security through graphical or command line interface.

The centralized security architecture management console should be capable of being configured so that only authorized users can perform security administration tasks. Individual administrator privileges ideally should be capable of being of being limited such that administrative tasks can be set to parameters for a limited subset of the items being secured. This will allow for generation of a group, which is authorized to perform limited security tasks, commensurate with the business needs. The policy management system should perform all management activities over an encrypted, authenticated connection. An administrator should be able to perform administrative tasks from any location in the network.

The task of defining the roles or access policies (e.g., determining which people are administrators or can see sensitive information) should be separated from the task of applying these access policies to the information being protected. This allows senior

management to define a particular access policy, and then pass the job of implementation to an administrator who cannot change the policy.

The centralized security architecture should provide an end-to-end secure tunnel for all user-to-web application communication. This tunnel provides an encrypted, authenticated connection for all network transactions.

It ensures that all data passed over the network remains secure and private, regardless of who accesses the network. Further, it enforces access control on all communications through these secure tunnels. The centralized security architecture should support standardized naming and directory services, which it uses to manage the namespace of protected information. This service can be used by an organization as a general-purpose directory service.

The centralized security architecture should support logical web namespace, in which content is accessed through a URL Authorization should be used from within most application development environments to provide application access to the authorization service based on objects. The objects should be a protected. The objects the system should support are as follows:

- *Web Objects* – These objects represent anything that can be addressed by a URL. This includes static web pages (e.g., index.html) as well as URLs that are converted to database queries or some other type of application invoked by a web-to-application gateway.
- *Network Application Objects* – These objects represent Transmission Control Protocol (TCP)-based applications (e.g., Telnet, legacy client / server or database) and map to the TCP network addresses (i.e., ports) being used by the application.
- *Data Objects* – These objects represent any information accessed by the application that is limited to specific user or group access.
- *Management Objects* – These objects represent the management activities that have the ability to be performed via the management console. The objects represent the tasks necessary to define and map users and to a set of security policies.
- By the use of these objects the system promotes the delegation of management activities and limits an individual's ability to set security policy to a subset of the protected object space or hierarchical structure.
- *Customer Defined Objects* – These objects represent customer-defined tasks or network resources that should be protected by applications that are using the fine-grained system. This allows the user to define objects that are to be protected. The rules define:
  - Which users or groups may access the information represented by the object.
  - Which roles may perform the task represented by the object?

The centralized security architecture should have the ability to manage dynamically generated URLs allowing an administrator to set access privileges for dynamically generated resources using the same policies that govern static resources.

The centralized security architecture should provide support for messaging infrastructures such as the International Business Machines (IBM) MQSeries.

The centralized security architecture should be capable of being used to create a secure tunnel between messaging clients and servers. The system should trap communications from the messaging subsystem and tunnels the network traffic without changes to the messaging application.

The centralized security architecture should be integrated with the messaging servers to implement fine-grained access controls in the messaging application.

The messaging applications should be capable of being directly integrated with the centralized security architecture tunneling services.

The centralized security architecture should provide its own tool to manage the entire infrastructure.

The centralized security architecture should use industry standard protocols such as, Secure Socket Layer (SSL), LDAP, and TCP-based Remote Procedure Call (RPC). It should be completely compatible with existing network infrastructure and firewalls.

The centralized security architecture authorization support should be capable of being added to applications being developed for UNIX and NT/Win 95 systems, CORBA-based tools (e.g., Iona or Visigenics), Powerbuilder, and SAP. The system should provide a Java interface.

The centralized security architecture should provide integration with Microsoft's Active Directory and Domain Security Services.

The centralized security architecture should provide security for legacy applications (those that cannot change) in two different ways:

- Remote access and client applications should provide a common authorization and data security service for existing TCP-based applications. This includes Internet applications such as Telnet, e-mail, as well as database client server applications.
- The centralized security architecture should provide security for databases. Remote Access and Client based software should secure existing database clients. Database clients running on a Win95 or NT system will use the TCP protocol to communicate with the server.

  The system should be capable of being integrated with either a RACF or ACF2 system. It should be capable of being integrated with system RACF/ACF2 services to provide an alternative to the centralized security architecture password or public-key certificate based authorization mechanisms. RACF or ACF2 user identity should get mapped into a set of centralized security architecture credentials for authorization checks.

4.4. Security Management

The SFA Security Framework allows two levels of security precautions.

1. It will protect the SFA network perimeter from intrusion and unauthorized access.

2. The SFA Security Framework will provide fine-grained proxy services that will authenticate, authorize, and control access to isolate activity between the two network interfaces, external and internal, by shutting off all direct communication between the two network interfaces. Network packets are never passed between these two interfaces.

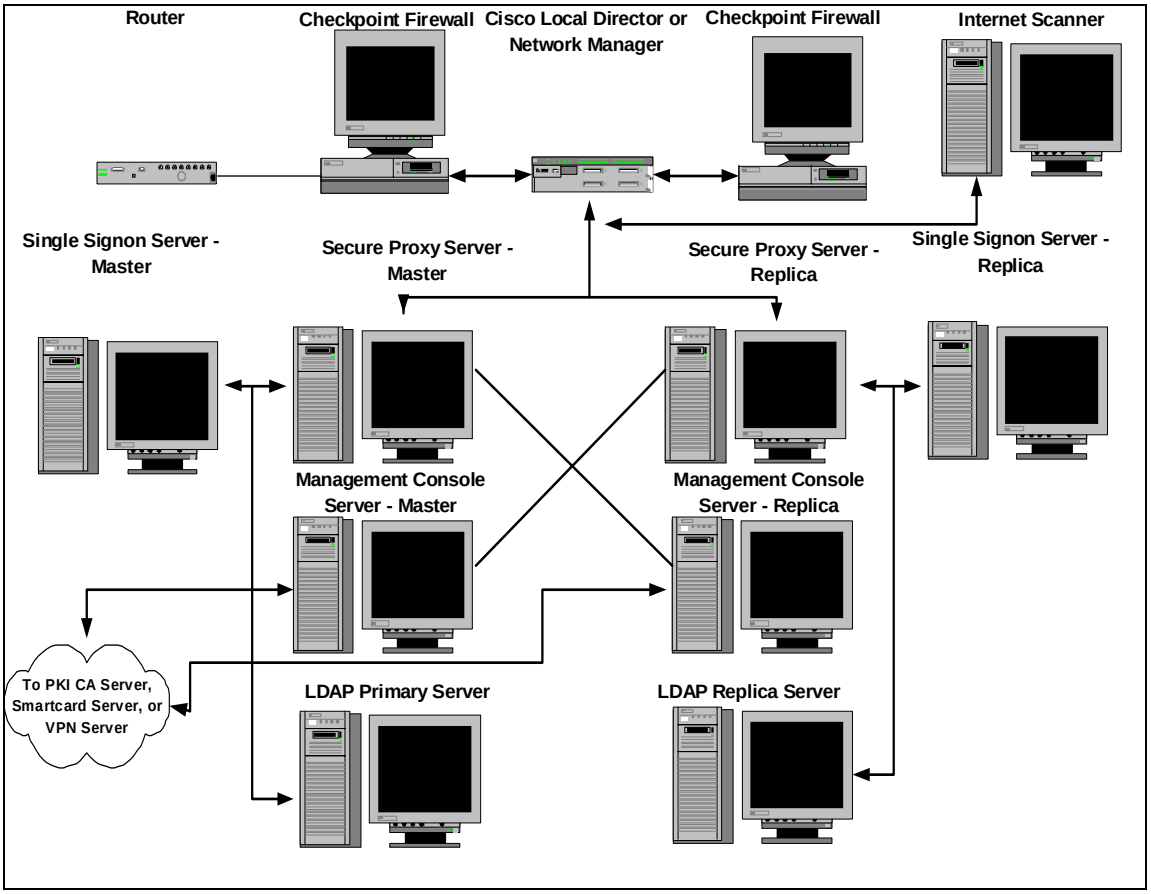

Figure 1 - Primary and Replicated Servers Layout

VPN Access

The SFA Security Framework should provide Virtual Private Network (VPN) services for remote users (replacement / augmentation for dial-in), extranet partners, vendors, service providers, and relationship based business associates.

Single Sign-on

The SFA Security Framework will contain all the underlying services responsible for ensuring a secure environment for Extranet, Internet and Intranet access, including single sign-on functions enabling users to identify and authenticate only once for access to multiple sources.

Global Directory

The SFA Security Framework will support Relational Database Management System (RDBMS)-enabled user databases as well as LDAP-enabled directory and registry functions that will contain lists all the valid users, groups, organizations, and password information necessary to provide inclusive single sign-on functions. The LDAP directory structure will contain an account entry for all valid security entities within a SFA domain. The SFA Security Framework will work directly in conjunction with the existing LDAP services supporting current systems.

Unified Administrative Interface

To create a secure domain, all functions provided by the SFA Security Framework should be administered via a single interface. This administrative interface will specify how the requesting user (no matter where located) will be allowed to participate in SFA's secure domain.

Application Protection

The SFA Security Framework will provide application security and authorization through integration with CORBA, Java, and Legacy applications via standard and customizable APIs.

The SFA Security Framework will protect internal SFA applications from misuse. Based on identity, each user is granted permissions to access limited types of data, files, and applications and can communicate only with designated resources.

Access Control Policy

The access control rules will shape the SFA security policy. The SFA Security Framework will provide sophisticated access controls defined through measures such as time, day, user groups, network groups, network interface, inbound & outbound authentication, and encrypted tunnels

Administration of Access Rules

The SFA Security Framework will have administration capabilities via a centralized management interface utilized to define and maintain access rules. Security administrators can set security parameters, control access, and monitor activity through this interface. Access rules let the security administrator control connections based on time, day, user groups, network groups, network interface, inbound & outbound authentication, and encrypted tunnels.

Remote Management

A remote management capability is necessary for network administration. The configuration of remote sites from a centralized location provides an additional layer of administration and

control of information security. The framework should provide such capabilities coupled with strong authentication and VPN service.

Delegated Administration of users

Analogous to the need for remote administration, the delegated administration of users is essential for efficient systems management. Management of users inside and outside SFA should be delegated to an infrastructure at the lowest common denominator, such as an academic financial administration group.

Event Monitoring and Alarm Generation

One of the most important requirements of the SFA Security Framework is the ability to monitor and respond to unauthorized activity. The Security Framework provides event monitoring, logging and detection of multiple types of activities. Implementation of the Security Framework allows detection when an event occurs that violates the system's security policy, generates alerts, and allows administrators to determine how to respond to the attempt.

4.5. Security Policy and Standards

Consistent Security Policy Management

The requirement is to be able to define a consistent security policy across different applications. The enabling pieces that make this possible are not only the same API, but also the use of equivalent credentials and entitlements, equivalent namespace for the protected objects, and the ability to attach the same policy definitions to the protected objects of different applications.

Centralized Security Policy Management

For the ease of administration and audit of policy definition, one should be able to centrally manage the policy for different applications. From a central logical point one should be able to view the complete set of privileges, roles, and entitlements given to an individual or group. One must also be able to quickly remove access rights that had been previously granted.

Flexible policies

There are many different businesses with different information risk management models. As such it is critical that any solution not favor one security policy model over any other model. For example, the system must equally support an "everyone but you" and a "least privilege" model.

Integration with legacy policy frameworks

In many cases, the modern applications will have to integrate and co-exist with existing SFA legacy applications. These existing applications often make use of standard or custom-developed authorization databases, like RACF, RDBMSs, OS / filesystem, etc. Through a common API, the authorization framework should be able to define exits outside of the application (external sources of authorization) that allows existing / legacy authorization engines to determine the access control decisions. The implementation should allow for transparent migration to newer / other authorization frameworks.

4.6. Security Awareness

Currently, SFA does not provide a general security awareness program. Several of the existing contracted companies offer services to develop and implement this type of campaign. SFA is encouraged to deliver a comprehensive awareness program as part of the ITA implementation. Distribution of the existing policy documents created and reviewed by SFA / KPMG provide an entry-level program for new and existing security managers, but a formal training program is needed to ensure individuals are aware of security, privacy, fraud, and audit requirements. Such a program can be instituted in conjunction with employee orientations and should at minimum require the employees to sign an acknowledgement of awareness as well as a non-disclosure / confidentiality agreement.

4.7. Security Administration

As SFA's IT systems proliferate to support necessary business processes, users and ultimately, administrators are faced with additional overhead resulting from users having an increasing number of systems and applications required to accomplish their job functions.

Users typically have to sign-on to multiple systems, necessitating an equivalent number of sign-on dialogues, each of which may involve different usernames and authentication information. For an individual user this may entail signing-on successively to:

- Single or multi-user operating systems
- Network- services
- Desk-top applications packages
- Work group packages
- Application systems
- Business applications packages
- Corporate databases

In today's environment each of the above system requires the user to remember and enter a different user ID and password for authorized access. Users often simplify passwords or write passwords down, both of which compromise security.

The number of users, systems, and applications significantly compounds the administration of user IDs and passwords for these systems.

The answer to this dilemma is to provide an infrastructure that permits a user to sign-on once while obtaining access to all of the required systems. The goal of Single Sign-On (SSO) is to eliminate the need for manually signing on to different systems by providing a single, automated process for identifying and authenticating users. That applies to all systems to which they have access. With SSO once users are successfully signed on, they gain access to the information resources they need without further manual intervention. SSO is an achievable goal, however, incremental milestones may be required (e.g., reduce log-on credentials from 8 to 6, 6 to 4, etc) depending on the complexity of the systems each user accesses. Even incremental improvement, with reduced log-ons results in cost savings via reduced administration time for account creation and maintenance.

To achieve SSO and fine-grained access control, SFA must create single or multiple secure domains. To create a secure domain within the system, the administrator specifies what users will participate in the secure domain group and where the business logic, data, links, or documents to be secured are located. The system then takes care of the underlying network issues and security precautions. It is implied that business logic will come in many forms, not limited to, but including CORBA objects, Java applets, web pages/sites, and partner or customer business logic elements to support nimble and progressive marketing initiatives.

The system is initially configured to include a basic set of system users in the directory. The administrator utilizes a central management console to add secure domain user and group accounts to the directory. A user is authorized to participate in the secure domain as soon as the administrator creates a directory entry for that user.

Typically, the user logs into the secure domain and requests to be authenticated. The security server sends back the user's authentication credentials, or security ticket. This ticket contains the user's identity, and the groups and organization to which the user belongs. A client uses this ticket to authenticate itself to a server. The ticket proves to the server that the client is legitimate. When the user tries to access a secure document via the access manager, the access manager will compare the authorizations contained in the user's ticket with the permissions assigned to the document. If these permission settings match the user's credentials, the access server gives the user access to the document.

On the client machine, a standard web browser such as Netscape Navigator or Microsoft Internet Explorer uses the system as a secure proxy. The secure client secures all HTTP traffic between the browser and the Access Manager.

The access manager controls the resources. This function ensures the integrity of the users and their actions. The Control Panel provides management access to all providers within the centralized security architecture. A secure object is an object that is protected by the system access control mechanism. A specific permission is assigned to web objects by defining the object's Access Control List (ACL). An object's ACL defines:

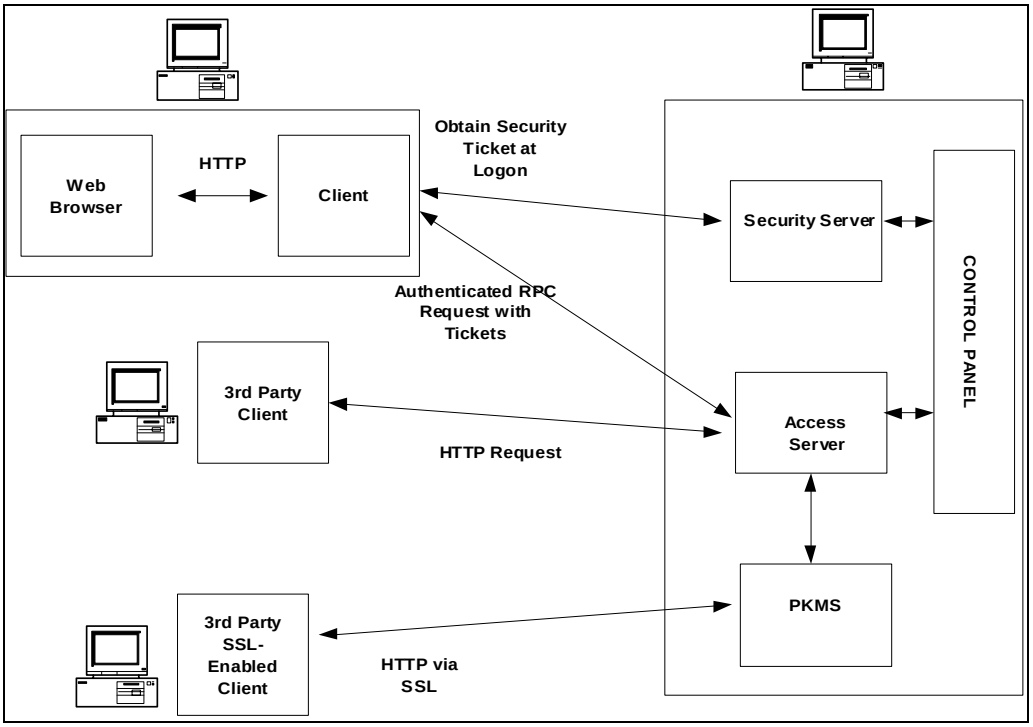

Figure 2 - Access Control via the Access Server

Permissions are assigned to individual users, special groups, or the entire organization. The ACL Manager provides an easy way to set and maintain ACLs. The ACL employs a mechanism to set global permissions so that permissions do not have to be set for every file or directory. The operations that can be specified include standard ACLs such as read and execute.

The security administrator should have at least two primary responsibilities:

- Assign credentials to users.
- Set ACLs on secure objects.

The security administrator has the capability to maintain a list of the users who can participate in the secure domain. The users can be listed by their name, password, or the organization / group to which they belong. User account information is stored in the security database.

The security administrator function is capable of setting the access controls on all web objects. He or she is able to tag each object file with the specific credentials required by any user needing access to this object. These credentials, called an ACL, are permission bits that define who can access any given object and what actions are allowed on this object. All groups of users to have viewing privileges can be designated for an object, but allow only one group of users to modify the object.

A browser will either communicate to the Access Manager via SSL V3 or a thin client interface where the system client interface provides a transparent security function that

authenticates and encrypts communications from a client desktop to the web-site or other TCP based server applications. The desktop client provides a VPN function between the Internet-based service and the client to avoid the client from being used as a router when connected to the Internet. The Client interface requires no browser setup or application configuration. User authorization (Access Control) is enforced and this service ideally will be installed and configured in the same location as the secure web server(s) and other application services. The system console manages the security policy.

The underlying mechanism used a centralized security architecture is grounded in both Federal and industry standard based technology. This includes functions that include but not limited to DCE, PKI, Common Data Security Architecture (CDSA) and CORBA interfaces.

4.8. Security Development

The SFA Security Framework should provide for a robust Authorization Framework to facilitate easy integration into legacy applications.

Web, CORBA & MQ Integration

The Authorization framework should be capable of consistent security policy across web, CORBA and MQ applications. An implementation of this requirement should make use of a common API model, the use of equivalent credentials and entitlements, equivalent namespace for the protected objects, and the ability to attach the same policy definitions to the protected objects of different applications.

API Support

The Authorization Framework should support a flexible cross-platform Application Programming Interface enabling applications to interpret and enforce access control policies.

The API should be able to express: "Can a user perform a particular operation at a certain point of the code?" In some cases, application specific state has to be communicated to the evaluator. In other cases, application specific credentials have to be communicated to the program to make the decision.

API Interface to Multiple Languages

The Authorization-API must be accessible from within different language environments. To ease the portability, the basic API should be defined in ANSI-C. Additional wrapper APIs can optionally be defined in higher-level languages, such as Java.

The API should provide support for a variety of languages and middleware interfaces. Some of the language and interface formats CORBA / DCE Interface Definition Language (IDL), serialized Java, Structured Query Language (SQL) / ODBC / TDF-vendor specific data stream format, ADL / Extensible Markup Language (XML), etc.

API Simplicity

It can not be stressed enough that the API should be as simple as possible, and that the choice of security flavor should be hidden as much as possible. Specifically, the API should hide all the issues related to management, storage, caching, replication, attribute certificate formats, authentication methods, etc.

A number of application frameworks allow for the transparent addition of access control points. Examples are CORBA interceptors, MQ exits, and dynamic URLs. The Authorization-API should be defined such that it enables transparent use of access control points.

API Components

The authorization framework may work with different type of evaluators based on the kind of policy definition governing that object which is probably related to the kind of protected objects. The essential components of the information exchange between the program and the authorization framework may include the following areas.

Server's Credentials

The program that makes that makes the actual Authorization-API calls is also subject to access control itself. In order for the security framework to determine whether the program is permitted to use the facility, a security context has to be shared between the program and the framework.

In most cases, the security context of the calling program is implicit. That is, the implementation of the API includes the integration with the desired security framework to establish the context.

Client's Credentials

When the client calls the Authorization-API to inquire about its abilities / capabilities, the caller and requester's identity is the same. When the second tier, i.e. a server, calls the Authorization-API, the requester's identity is that of the client. The Authorization framework should be capable of enforcing access policies on resources based on the initiator's credentials, the intermediate's credential or a combination of both in conjunction with the established delegation policy of the Authorization Domain.

Protected Object Identification

In order to externalize the policy administration of an authorization decision, the objects must be identifiable. Some naming convention has to be established to uniquely distinguish the evaluations. The name "protected object" is used to identify a particular decision point.

It makes sense to look at established namespaces for the identification of protected objects, like URLs, LDAP / X.500 DNs, hierarchical file-directory like schemes, etc. Many of these schemes have an implicit hierarchical structure that may be used to ease the policy management.

Requested Operation on the Protected Object

Many existing access control systems describe the security policy in terms of permitted operations on protected objects. File systems commonly have permission sets that include operations like read, write, delete, etc. The set of operations is specific for the type of protected object, and should theoretically be customizable per type of protected object. Although conceptually an operation could be viewed as "application specific state" or as an extension of a named hierarchical object, it is widely used in existing ACL implementations. A separate interface that deals with an explicit operation may be warranted. The authorization framework and administration tools should be able to deal with customizable operations.

Application Specific State for the Evaluation

There is clear requirement to communicate application specific state such as "requested amount to withdraw", to the evaluator through the authorization framework in a generic fashion. It may be possible to leave the exact format to the implementation of the evaluator, which would be implemented as an external authorization engine.

Middleware Support

The Authorization Framework should implement the CORBA Level 1 (transparent security for CORBA apps) and CORBA Level 2 security features.

The Authorization Framework should be capable of enforcing Access Control policies on Java Applets and Servlets.

The Authorization Framework should be capable of enforcing Access Control policies on ActiveX components and resources in a Microsoft environment.

MQ

The Authorization Framework should be capable of securing MQ applications, including the capability for authentication; access control to MQ based services, privacy and integrity of MQ communications as well as the capability for MQ applications to make fine-grain access control decisions.

Java

The Authorization Framework should be capable of providing access control to EJB components.

The enterprise architecture diagram at the end of the section is in common use with a variety of authorization tools in multiple locations. It can be modified, and used as a starting point for the SFA integration. It is shown to be generic, but will support the following four application categories:

- Applets

- Servlets (J2EE compliant Application Servers)
- CORBA Servers
- EJB Components

Several categories have been identified for which adequate interfaces would need to be defined. The identified categories are:

- Registration and Initialization (as necessary)
- Authentication
- Credential Management
- Simple Authorization
- Entitlements
- QOP
- Delegated Administration
- Auditing

The above categories are a solid starting point for this architecture. Further analysis and design is required to refine this authorization architecture. These may be augmented, others may be removed or the semantics redefined as interact begins with the developers and the different application groups.

As may be evident from the architecture diagram, the following would apply to the above interfaces:

- Java interfaces with appropriate packaging.
- Possibly might require a bootstrapping object (singleton) that returns objects of the appropriate interface.
- There will be different implementations of the above interfaces for the different application categories. An attempt will be made to provide a very thin layer that is application category specific, with most of the functionality being implemented within category independent package (classes).
- The different implementations may use the proposed Authorization Service in conjunction with already available Commercial-Off-the-Shelf (COTS) solutions such as possibly a CORBA Level 2 solution.

At the heart of this framework would be a service (Authorization Service in the diagram) that provides the necessary vendor, technology, domain, application, and platform insulation. The following apply to the design of this service:

- The service will have a well-defined interface - either CORBA or Remote Method Invocation (RMI).
- The internal implementation of this service will use well define "service" interfaces. These "service" interfaces may be nothing more than a reflection of the client interfaces.

Adaptors will be provided for the above "service" interfaces. These adapters will have the following properties:

- Abstract vendor implementations
- Abstract technology, domain
- Abstract application specific nuances
- Abstract any platform specific details (if necessary)

The following diagram depicts an example Security Framework to facilitate easy integration into legacy applications.

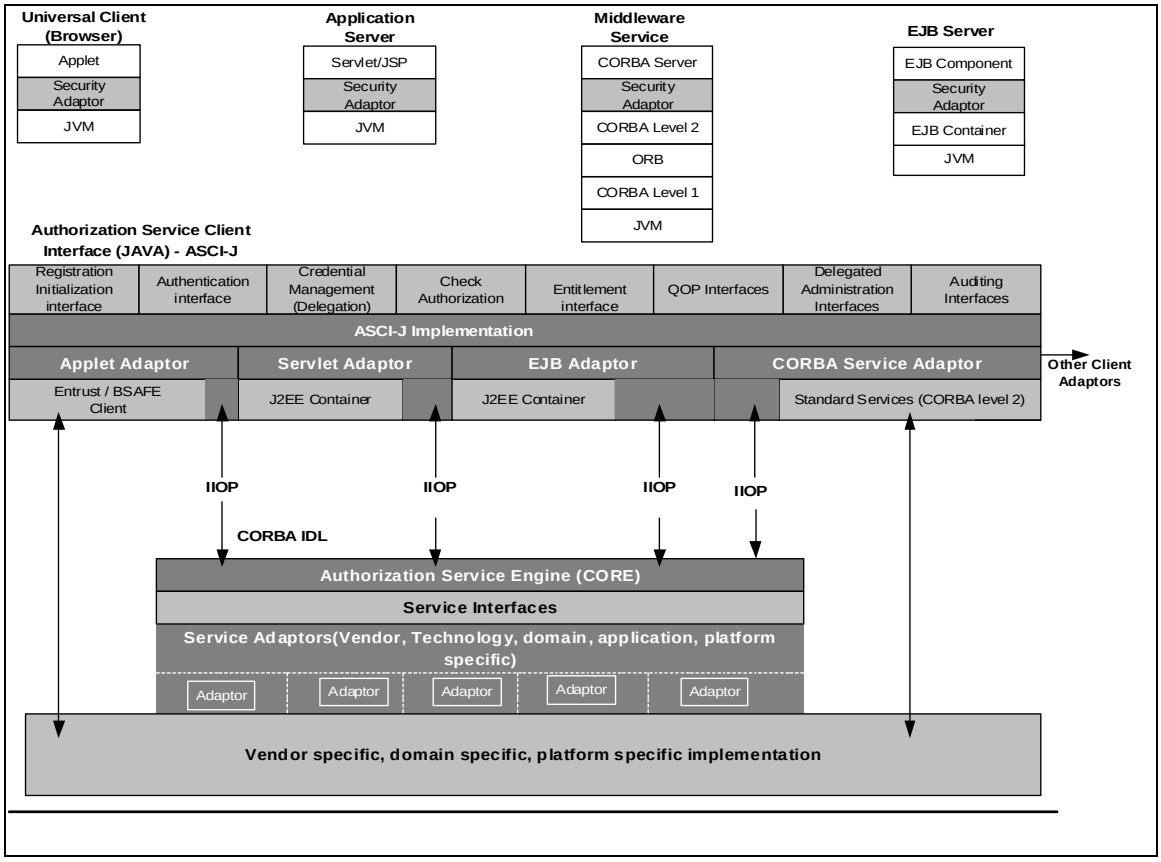

Figure 3 - Example Security Framework for Legacy System Integration Security Operations

All system server(s) should be capable of being replicated to provide a solution that scales to the particular network. The architecture should provide functions to back-end applications and web servers enabling replication, scalability, high availability, and load balancing. This feature should allow SFA to augment the scale of a particular network to increase resources, achieve high availability for users, and protect the site from sudden server failure. The system should provide fail-over capabilities. For example, there should be the capability to replicate each process within the system. It should place the resources of a heavily accessed web site in a state of high availability. Users should be able to concentrate on the information and services provided by the web-based resources and not its physical location.

The system should provide management services that perform load balancing across replicated servers for improved performance and fault recovery. These replicated servers consist of web servers supplying mission critical content, either as static web pages or via gateways to existing business applications. Ideally they should be capable of being replicated. The system should be capable of providing security and availability services from one central management location, with multiple control and failover locations for redundancy, and delegation of authorization authority to business component owners.

The system should be able to be subdivided across multiple servers, images, and domains, where database and access functions can be split for load balancing and failover. This will provide the capability of selected functions to be replicated, ensuring that the resources are available when users need them. Further, this will allow the security functionality to compliment the network traffic flows, patterns, and requirements. To aid in this effort the security policy for the organizational domain should make use of a hierarchical namespace, where that policy supports and an inherited tree structure, unless overwritten with an explicitly attached named policy template. This ability to structure a policy with an inheritance function and a named policy template makes the management of the policy easier and more scalable. The system should be capable of supporting multiple management consoles that can be deployed within the enterprise. It should support administrative accounts that can be set up to permit different business units to manage appropriate pieces of their own security policy. In this way, the management of the security policy can scale throughout the enterprise.

The distribution of administration responsibilities within a secure domain is called management delegation. The need for management delegation generally arises from the growing demands of a large site containing many distinct departmental or resource divisions. Typically, a large object space can be organized into regions representing these departments or divisions. These domains or divisions are obviously better maintained by an individual who is more familiar with the issues and needs within that entity. This replication should be managed by the system, so it does not add to the administration of the running system. Additionally, replication should not be constrained by geographic boundaries, so the resources protected by the system can be geographically separated.

4.9. Security Services

Security Services supports re-useable common security architecture components. Within the VDC, the majority of the security tools and products purchased (e.g., Firewalls, routers, Virus detection) are executed in a standard re-useable fashion. The bulk of these services are for defensive security. However, to gain the maximum leverage off of existing development resources, vendors, and contractors SFA must use a common, reusable security framework. These tools allow SFA to have a consistent security development, configuration management, software distribution, testing, and production support environment. The ability to rapidly adapt new systems to this security framework will allow SFA to roll secure applications out to meet the business needs.

4.10. Security Infrastructure

SFA Security Infrastructure Security will offer maximum security for the various applications. It will offer comprehensive security services for all TCP / Internet Protocol (IP) and legacy applications, presenting an implementation of a transparent portal gateway. In addition to the existing security infrastructure located at the VDC, the following infrastructural components offer the ability to enable applications for Internet transactions, code API interfaces securely into applications, and handle large volumes of users while moving them closer to SSO.

The following diagram illustrates an example of a security infrastructure which provides these services.

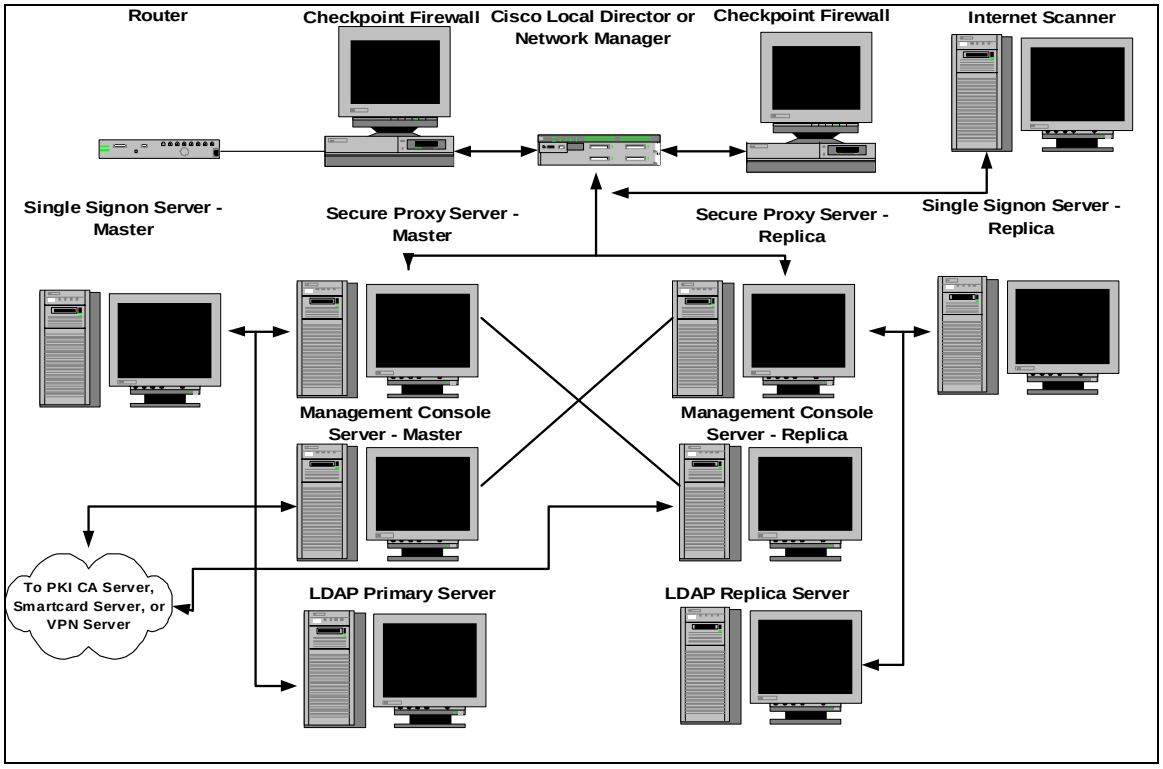

Figure 4 – Example Security Infrastructure and Services

Global Directory (LDAP)

LDAP uses the X.500 information model. The core X.500 model is of a tree of entries, each of which contains information about a particular object. Entries are composed of attributes, which have a type and one or more core values. Each attribute has a syntax that determines what kinds of values are allowed in the attribute. In the tree, each entry is uniquely named relative to its siblings by its relative distinguished name consisting of one or more distinguished attribute values from the entry. The concatenation of all the relative distinguished names from the root of the tree to a particular entry is that entry's distinguished name, which is globally unique.

Migration of existing RDBMS user-id database to the Global Directory is possible, enabling use of existing investment / data available in DB2 and Oracle Databases.

LDAPv3 is defined to be a client server protocol, and the server can be provided in any manner. There is no requirement to use LDAP to access an X.500 directory. It is important to remember that LDAP does not create a complete, enterprise-wide directory solution. LDAP is nothing more than its name implies, a lightweight directory access protocol.

A standardized schema and access control in LDAP is required in a distributed environment offering multiple directory services. Each of the LDAP front-end servers to these directories will have an individual network address. In order to make use of all of these directories, authentication and authorization services will need to know and maintain: the network location (IP, fully-qualified domain name, etc.) of each LDAP server, the username and password to use in accessing each server, and a schema definition for each server.

To switch from one directory to another, it may be necessary for the user to reconfigure his / her application in order to plug in the applicable address, authentication, and schema parameters. This creates an intranet consisting of a collection of independent LDAP islands; a collection of directory services that are isolated from each other but have the common characteristic that they are accessible using the LDAP protocol.

5 Gap Analysis of Current Infrastructure

5.1. Business Assets

This section quantifies the Information Security Gaps between the current SFA environment, and the proposed SFA security environment. System Level Gaps tend to fall within one of two major subheadings:

- Defensive Security Measures
- Enabling Security Measures

Systems that were evaluated for the Gap Analysis are for the Release 1 applications include:

- IFAP
- Schools Portal
- Intranet Release 2.0

Systems that were evaluated for post-Release 1 include:

- Campus Based Systems (CBS)
- Central Processing System (CPS)
- Direct Loan Consolidation System (DLCS)
- Direct Loan Origination System (DLOS)
- Direct Loan Servicing System (DLSS)
- Federal Family Education Loan (FFEL)
- Multiple Data Entry (MDE)
- National Student Loan Data System (NSLDS)
- Post-secondary Education Participants System (PEPS)
- Recipient and Financial Management System (RFMS)
- Title IV Wide Area Network (TIVWAN)

5.2. Risk Management

The Department of Education SFA systems provide adequate security measures for securing short term and long term applications housed within their data centers. The Modernization Partner with the Department of Education is working towards performing formal Risk Assessments and Risk Management programs. Further, there are software packages and software products that support methodology based Risk Assessments.

Appendix A, Information Security Core Technology Status is a matrix that depicts specific, case by case analysis of current security products purchased and implemented. Appendix B, System Technology Risk Matrix defines the technology that exists on each SFA platform. These documents should be considered living, working documents and completed by the

CSC Staff in the VDC. Appendix A clearly identifies the areas where there is no security product in place.

Appendix B is the template for a Technological Risk Assessment. The individuals conducting the Risk Assessment will evaluate each of the SFA technology suites, assess known vulnerabilities known for each of these technologies, and provide recommendations and minimum security baselines, product by product, for ensuring consistent, secure installation and configuration of each product. This will provide SFA with a consistent "build" model which not only benefits Information Security, but also configuration management, software distribution, and data integrity controls.

5.3. Security Strategy

Information Security is generally broken down into two major disciplines, Traditional Defensive Measures (Blocking and Tackling Intruders) and Enabling Measures (eCommerce, promoting business functions, enabling remote users). SFA's technology, management processes and technical staff has implemented a sound defensive security posture.

From a Security Strategy perspective, SFA management and CSC data center management have a solid program to continue to grow security. This effort is part of that growth and maturity process.

The primary gap in the strategy (which is a recognized gap) is the lack of a comprehensive enabling Standard Security Framework. This has resulted in application and system vendors having to implement security integrity controls and authorization in individual proprietary fashion. There are several problems associated with these non-standard proprietary point solutions. The emerging internet / extranet infrastructure has introduced new forms of access control challenges.

With extranets the application audience has changed, audiences are not limited to internal corporate users but today encompass suppliers, trading partners and customers. The untrusted nature of extranet constituents has necessitated tighter end-to-end application security and fine-grained authorization.

With the changing e-business landscape security architectures have to exhibit the scalability, flexibility and adaptability to support emerging business models.

A common security framework is needed to provide credentials that are trusted across organizational boundaries, establish effective access control and authorization mechanisms for diverse extranet user constituencies and enforce consistent security policies on applications. A standards-based security framework helps organizations to implement a scalable security architecture that best meet the organization's security policy while significantly lowering development, deployment and administration costs.

The SFA Security Framework addresses several security paradigms that are synergistic in nature: fine-grained access control, authorization, authentication and single sign-on potential. The combination of these functions within a single entity, conceptually referred to as an

enterprise security portal will provide SFA with a secure, reliable, and available framework to its varied applications, web sites, and databases.

5.4. Security Management

The Security Management team at SFA is motivated to resolve system deficiencies and advance the entire Information Security Program. Penetration tests, policy development and overall information security supports the growth and maturity of the SFA Information Security Program. The CSC management for the VDC data center is reasonably executing security solutions provided and responding to solid controls security, business resumption, availability, and serviceability. The recommendation is to continue to grow programs and develop the overall security posture.

5.5. Security Policy and Standards

The Modernization Partner and SFA have created and will continue to refine Information Security policies. These policies augment Department of Education policies. These policies provide a sound business basis for security policy and awareness, but not technology specific standards for configuration. Plans are initiated to continue to develop these specific standards. SFA should continue to close the gap between business policies and solid technical standards. SFA should continue to complete Information Security policies, which offer users, developers and managers sufficient technical design detail to execute security remedies on operating systems, databases, networks, and associated devices.

5.6. Security Awareness

A solid Security Training and Awareness program was not evident at SFA. However, all developers, managers, and employees appeared motivated to institute a solid security posture for SFA.

5.7. Security Compliance

5.7.1. Network Security

The overall network perimeter is protected via multiple layers of network security. Cisco Router level security (ACLs) are utilized on critical Intranet environments, network sniffers are installed to protect against denial of service attacks, and finally all network traffic accessing the Internet is protected via a Firewall. All products involved are first in their class according to industry statistics and think tank groups such as Gartner and Giga. These solutions clearly resolve the majority of the network security issues.

CSC and the Modernization Partner are already working towards implementation of Penetration Tests and a CERT team. Final execution of these two functions is critical to constantly test environments against new vulnerabilities and exposures. Further, these two functions are key to solid business resumption, business continuity and availability execution plans.

Tripwire is currently in use in some of the data center areas. However, more robust Network Mapping, Active Intrusion Detection and Logging tools are available on the market to actively detect and react to real-time penetrations from hackers. Suggest an RFP be initiated to pursue products and tools required. Suggested products include Netranger, Risk Manager, eSecurity, ISS Realsecure, and Ballista.

5.7.2. Host Level System Security

Tripwire is currently used in a limited capacity for file access monitoring. Tripwire is a specialized product with the purpose of monitoring access to designated critical files. However, more comprehensive host and network-based intrusion detection systems, policy compliance assessment, centralized log collection and decision-based reaction tools are available.

The security posture on SFA host operating systems is currently inadequately monitored. BMC's Control SA product was purchased to assist with system security requirements, but this product is targeted at security management on mainframe applications. Distributed computing environments present a greater level of risk to the organization and should be monitored accordingly. Host-based intrusion detection products and policy compliance assessment tools are available and highly recommended. Such tools monitor and assess the host in accordance with the established Information Security standards of configuration.

5.7.3. Security Standards of Configuration

A set of written documents is needed outlining policies and procedures for the configuration of all SFA Information Systems to ensure minimal security exposure. These standards of configuration are needed at varying levels, from general standards to operating system specific standards to application-level standards. The establishment and implementation of such standards enables the SFA to measure the level of security compliance within the organization. Such standards should be applied to all information systems connected to SFA networks regardless of ownership. In addition, establishment of minimum standards, in correlation with policy compliance assessment tools, drastically reduces lost resource time necessary for conducting system audits.

5.7.4. Database Security

SFA has purchased a multitude of database systems. Mainframe and Midrange systems level security is implemented on databases via RACF and Ca Top-Secret. Client Server RDBMS security is virtually nonexistent, with the exception of one Oracle system on the PEPs system. The majority of the client server databases are provided with security features, documentation, and tools.

Recommendation is for DBAs to expand scope of work for deliverables to allow for the additional time to implement and execute already purchased security on SFA databases.

5.8. Security Administration

The primary gap in the strategy (which is a recognized gap) is the lack of a cohesive Enabling Standard Security Framework. This has resulted in application and system User ID Administrators to implement a variety of security control schemes, UserID databases, and access rules, which are inefficient. There are several problems associated with these proprietary point solutions:

Users' access rights are defined in several places and within several systems within a corporation. Customers and users are unable to possess a coherent, simple access point to systems. Further, auditors are unable to get a complete view of a user's capabilities and thus are unable to determine any risks associated (e.g., with conflicting privileges). If an employee leaves the organization, his / her access rights need to be deleted at several places. This task is very difficult to track and manage and may lead to security vulnerabilities.

Since authorization definitions are also not standardized, each user, partner, or vendor ends up defining it in a way that is most suitable to their application and thus requires their own administration tools to manage those. Some of the application authorization information is generic and may need to be shared by a number of applications. Currently this information needs to be duplicated at several places, which may result in inconsistencies.

5.9. Security Development

The Security Services offered currently lack a consistent Security Framework to enable applications, Internet Portals, and web content. Each implementation instance or system accomplishes application and web content security in a different fashion. A common Security Framework will speed application developer timeliness, improve efficiency of security, and offer customers further ease of use in terms of personal UserID maintenance.

5.10. Security Operations

SFA Security Operational support is provided by CSC. Documentation regarding the operational aspects of security was not provided as part of this study since it is outsourced to CSC. However, as a result of interviews, discussions with technical staff, and a review of documents it is concluded that Security Operations actively employs all security tools, methods, and technology available. Therefore, all technology provided is put effectively into use which cost justifies security expenditure. More operational documentation is required to provide a full Gap Analysis of the Security Operations functions.

5.11. Security Services

Security Services supports re-useable common security architecture components. Within the VDC, the majority of the security tools and products purchased (e.g., Firewalls, routers, Virus detection) are executed in a standard re-useable fashion. The bulk of these services are for defensive security. However, SFA needs a common, reusable, security framework suite of tools to enable a consistent security development and production support environment.

5.12. Security Infrastructure

The attached Information Security Core Technology Status provides full details of the current Security Infrastructure. The infrastructure is managed by CSC and appears to be effectively designed from the defensive security perspective (Firewalls, Routers, Virus's, etc). Hardware and software purchased by CIO is getting implemented and executed reasonably. As gaps, architectures and recommended tools are defined, it is reasonable to assume that CSC will act upon the tools and implement as time / resources permit.

6 Glossary - Acronyms and Terms

6.1. Acronyms

For those that I did not know what they meant I deleted. Please compare with the original since they did not highlight as a change but rather got deleted.

Table 2 – List of Acronyms

Acronym	Description
ACL	Access Control List
API	Application Programming Interface
CBS	Campus Based Systems
CDSA	Common Data Security Architecture
CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CIO	Chief Information Office
COE	Common Operating Environment
CORBA	Common Object Request Broker Architecture
COTS	Commercial-Off-the-Shelf
CPS	Central Processing System
CSC	Computer Sciences Corporation
DCE	Distributed Computing Environment
DDD	Detailed Design Document
DLCS	Direct Loan Consolidation System
DLOS	Direct Loan Origination System
DLSS	Direct Loan Servicing System
DOE	Department of Education
EJB	Enterprise Java Bean
FFEL	Federal Family Education Loan
HTML	Hypertext Markup Language

Acronym	Description
IBM	International Business Machines
IDL	Interface Definition Language
IP	Internet Protocol
IFAP	Information for Financial Aid Professionals
ITA	Integrated Technical Architecture
LDAP	Lightweight Directory Access Protocol
MDE	Multiple Data Entry
NSDLS	National Student Loan Data System
PEPS	Post-secondary Education Participants System
PKI	Public Key Infrastructure
QOP	Quality of Protection
RDBMS	Relational Database Management System
RFMS	Recipient and Financial Management System
RMI	Remote Method Invocation
RPC	Remote Procedure Call
SA	Security Architecture
SFA	Student Financial Assistance
SQL	Structured Query Language
SSL	Secure Socket Layer
SSO	Single Sign-On
TCP	Transmission Control Protocol
TIVWAN	Title IV Wide Area Network
URL	Uniform Resource Locator
VB	Visual Basic
VDC	Virtual Data Center
VPN	Virtual Private Network
XML	Extensible Markup Language

6.2. Terms

Table 3 – List of Terms

Term	Definition
Access Control List	The context, in terms of such variables as location, time of day, level of security of the underlying associations, etc., in which an access to a security object is made. 1. Control over the flow of information between entities. 2. The prevention of access without access rights. Access controls the process of determining who is given access to a computer resource, such as database information, and how much information he/she can receive.
Access Control Mechanism	A list associated with an object specifying the access rights of subjects to that object. A set of control attributes. It is a list, associated with a security object or group of security objects. The list contains the names of security subjects and the type of access that may be granted. An ACL is a list of subjects that are authorized to have access to object(s). Usually, this list contains entries consisting of identifiers of users and groups of users and access rights. A list of entities, together with access rights which are authorized to have access to a resource. Discretionary access control mechanism associated with an object, consisting of a list of entries, where each entry is a subject identifier coupled with a set of access permissions.
Access Control Policy	Security safeguards designed to detect and prevent unauthorized access, and to permit authorized access in an IT product.
Active Content	A set of rules, part of a security policy, by which human users, or their representatives, are authenticated and by which access by these users to applications and other services and security objects is granted or denied. An access control policy is a set of rules that define the conditions under which an access may take place. A set of rules, part of a security policy, by which subjects are authorized and by which access by these subjects to objects is granted or denied.
ActiveX	WWW pages which contain references to programs which are downloaded and executed automatically by WWW browsers.
Andrew File System (AFS)	An AFS is a location-independent file system that uses a local cache to reduce the workload and increase the performance of a distributed computing environment. A first request for data to a server from a workstation is satisfied by the server and placed in a local cache. A second request for the same data is satisfied from the local cache
Applets	Software components which will be downloaded automatically with a WWW page and executed by Microsoft, Inc.'s Internet Explorer WWW browser. Small applications written in various programming languages which are automatically downloaded and executed by applet-enabled WWW browsers
Application-Level Firewall	A application level firewall is a system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.
Application-specific Proxy Servers	Application-specific proxy servers provide proxy service for a specific application (i.e., telnet). Are not readily available for services other than FTP, telnet, or the web.

Term	Definition
Asymmetric Authentication Method	Method for demonstrating knowledge of a secret, in which not all authentication information is shared by both entities.
Authentication	The process of verifying the identity of users through the use of an instrument such as a password.
Authorization	The process of granting access to a local or remote computer system, a network, or online information.
Biometric Access Control	Any means of controlling access through human measurements, such as fingerprinting and voice printing.
Browser	A client program used to interact on the WWW
Certificate	Security data sealed by an Authority. The certificate contains the security data and the seal.
Certificate Authority	Certificate Authorities (CAs) vouch for the identities of individuals and their certificates. The certificates of Certificate Authorities are signed by a Policy Certification Authority. CA is an entity or service that distributes electronic keys for encrypting information and electronic certificates for authenticating user and server identities used to create the encryption pattern.
CGI	The Common Gateway Interface (CGI) is the standard method used by web servers to provide a gateway to outside programs that are executed by the server in response to a user action.
Cyphertext	Data produced through the use of encipherment. The semantic content of the resulting data is not available. Note: cyphertext may itself be input to encipherment, such that super-enciphered output is produced.
Clear-text	Intelligible data, the semantic content of which is available.
Cookie	A cookie is a little piece of text that's sent to a web browser from a web site that the browser is viewing. What's in a cookie is usually a string of characters, unique to the user, that's generated by the web site. Later, when that individual goes back to that same web site, it can grab the cookie. A cookie can't be larger than 4K, and cookies can be read only by the web site that sent them.
Cryptography	The discipline which embodies principles, means, and the methods for the transformation of data in order to hide its information content, prevent its undetected modification and / or prevent its unauthorized use. Note: Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or methods is cryptanalysis.
Crypto-Algorithm	A well-defined procedure or sequence of rules or steps used to produce a key stream or cipher text from plaintext and vice versa.
Cryptographic Checksum	A one-way function applied to a file to produce a unique fingerprint of the file for later reference.
Data Integrity	The property that data has not been altered or destroyed in an unauthorized manner. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. The property that data meet an a priori expectation of quality.

Term	Definition
Data Encryption Standard (DES)	A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and government use.
Digital Certificate	A public key directory entry that has been signed or validated by a certification authority. Digital certificates are used to verify digital signatures.
Digital Signature	A coded message added to a document or data that guarantees the identity of the sender. Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.
DMZ	The "Demilitarized Zone" lies outside the perimeter defenses provided by the firewall but contains systems that are owned by a private organization. Common examples would be web servers and anonymous ftp servers providing information to Internet users.
DNS Spoofing	Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.
Dual Homed Gateway	A system that has two or more network interfaces, each of which is connected to a different network. In Firewall configurations, a dual homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks.
Electronic Commerce	The use of an electronic information infrastructure through which businesses can speed the exchange of information, improve customer service, reduce operating costs, and increase global competitiveness.
Encryption	Method of encoding information to prevent anyone, other than the intended recipient, from reading the information.
End-To-End Encryption	The protection of information paged in a telecommunications system by cryptographic means, from point of origin to point of destination.
File ACL Class	The property of a file indicating access permissions for a process related to the process' user or group identification.
Firewall	A security mechanism for controlling access between a private trusted network and an untrusted outside network (which might be the public Internet or some other part of the corporate network within an intranet). It is comprised of software running on general purpose or specialized hardware. A firewall is a combination of systems that enforces a boundary between two or more networks. A perimeter defensive mechanism used to provide control over data traveling between two or more networks.
FTP	File Transfer Protocol: (TCP / IP) the Internet application and protocol used to send complete files over TCP / IP services. An IP application protocol for transferring files between network nodes. The TCP / IP standard, high-level protocol for file transfer from one machine to another. FTP uses TCP. An IP application protocol for transferring files between network nodes. A TCP / IP application, service. And protocol for copying files from one computer to another. Before the server will transfer the files, it requires the client to provide a valid username and password. Anonymous ftp is used at public network sites. It allows file transfer using a standard username, 'anonymous " plus the user's e-mail address as the password.

Term	Definition
Generic Proxy Servers	Accept incoming connections, consult a table, and determine which connections are allowed, and makes the connection. Are usually part of firewall packages. Do not function in a one-to-many or many-to-many environment (i.e., clients cannot access multiple servers).
Gopher	Protocol designed to allow a user to transfer text or binary files among computer hosts across networks.
Hack	Any software in which a significant portion of the code was originally another program.
Hacker	Those intent upon entering an environment to which they are not entitled entry for whatever purpose (entertainment, profit, theft, prank, etc.). Usually iterative techniques escalating to more advanced methodologies and use of devices to intercept the communications property of another.
Hardened OS	Refers to an operating system that has had its attackable services / applications removed. The resulting operating system offers few vulnerabilities for hackers to attack, often used to construct firewalls. However, this process makes the operating system non-user friendly and somewhat proprietary.
Hash Function	A function that maps values from a (possibly very) large set of values to a smaller range of values. Hash is a mathematical function which maps values from a (possibly very) large set of values into a smaller range of values. Hash function transformation takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is, h = H(m)). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties.
HTML	The HyperText Markup Language. The mechanism used to create web pages.
HTTP (Hypertext Transfer Protocol)	The TCP / IP protocol for transferring World Wide Web pages across the Internet. The HyperText Transport Protocol. The native protocol of the web, used to transfer hypertext documents
IPSec	The IP Security (IPSec) Protocol, is a standards-based method of providing privacy, integrity, and authenticity to information transferred across IP networks. The Internet is subject to many threats, including loss of privacy, loss of data integrity, identity spoofing, and denial-of-service. The goal of IPSec is to address all of these threats in the network infrastructure itself, without requiring expensive host and application modifications. IPSec provides IP network-layer encryption. The standards define several new packet formats: the authentication header (AH) to provide data integrity and the encapsulating security payload (ESP) to provide confidentiality and data integrity.
IP Splicing / Hijacking	An attack whereby an active, established, session is intercepted and co-opted by the attacker. IP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer.
IP Spoofing	An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.

Term	Definition
Java	Programming language invented by Sun Microsystems, Inc. It can be used as a general purpose application programming language with built-in networking libraries. It can also be used to write small applications called applets. The execution environment for Java applets is intended to be safe, that is, executing an applet should not modify anything outside the WWW browser.
Key	A long string of seemingly random bits used with cryptographic algorithms to create or verify digital signatures and encrypt or decrypt messages and conversations. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message.
Key Management / Exchange	A method of electronically transmitting, in a secure fashion, a secret key for use with a secret key cryptographic system. Key management can be used to support communications privacy. This method can be accomplished most securely with public key cryptographic systems, which do not require the sharing of secret keys with third parties. Instead, a secret key is encrypted with a recipient's public key, and the recipient decrypts the result with his or her private key to receive the secret key. A variation of key management that is based on key exchange does not require encrypting the secret key.
Key-escrow System	An electronic means of reconstructing a secret key (for secret key encryption) or a private key (for public key encryption). The reconstructed key can then be used in a process to decrypt a communication.
MBONE	(Multicast BackBONE) A cooperative agreement among sites to forward multicast datagrams across the Internet by the use of IP tunneling.
Masquerading	Synonymous with spoofing.
Mimicking	Synonymous with spoofing.
Network Address Translation (NAT)	With the growing shortage of IP addresses, it has become increasingly difficult for organizations to obtain all the registered IP addresses they need. A network address translator solves this problem by dynamically converting between a re-usable pool of dynamically assigned registered IP addresses and the internal IP addresses used in an organization's intranet. This not only alleviates the IP address crunch, it also eliminates the need to renumber when an organization changes Internet service providers (ISPs). Some firewalls can provide NAT.
News (Network News Transfer Protocol, NNTP)	Protocol for Usenet news distribution. Usenet is a system for asynchronous text discussion in topic subdivisions called newsgroups.
NFS (Network File System)	A protocol and service that allows networked computers remote, transparent access to directories and files. The remote files appear to a user to be local. A protocol developed by SUN Microsystems, Incorporated that uses IP to allow a set of cooperating computers to access each other's file systems as if they were local. A protocol developed by SUN Microsystems, Incorporated that uses IP to allow a set of cooperating computers to access each other's file systems as if they were local.
NIS (Network Information Service) (Old Yellow Pages)	A service for networked computers, providing a single, shareable copy of common system and configuration files. It lets computers share system and user accounts. NIS client issues queries for the information stored on the NIS server. NIS server response is either requested information or no info response.

Term	Definition
NNTP (Network News Transfer Protocol)	The TCP / IP protocol used to transfer usenet news articles between two nntp servers and between a newsreader and an nntp server.
Packet-Level Firewall	A Firewall in which traffic is examined at the network protocol packet level.
PPP	Point-to-Point Protocol. A successor to SLIP, this protocol provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. See also SLIP
Protocol Gateway	A protocol translation mechanism for connecting (for example) an IPX network to an IP network (public or private). The term "gateway" is also sometimes used to refer to circuit-level and application-level firewalls.
Public-Key Security	Also known as asymmetric-key security or public-key encryption technology, this is a security mechanism for securely distributing encryption keys that are used to "lock" and "unlock" data across an unsecured path. Public-key security is based on encryption key pairs, in contrast to private-key security, which is based on a single, shared key. Private Key Cryptography provides an encryption method which requires both parties of a digital transmission to know the same key for encryption and decryption. A key used in an asymmetric algorithm. Possession of this key is restricted, usually to only one entity. The key, used in an asymmetric algorithm, that is known to only one entity. The undisclosed key in a matched key pair - private key and public key - that each party safeguards for public key cryptography.
RSA – RC2, RC4 (Rivest Cipher 2 and Rivest Cipher 4)	Generic name for an encryption mechanism developed by RSA Data Security that uses both a private and a public key. RSA is also used to verify user and / or server authenticity. The RSA public key algorithm invented by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman (RSA). RSA performs the key management process, in part, by encrypting a secret key for an algorithm such as DES, RC2, or RC4 with the recipient's public key for secure transmission to the recipient. This secret key can then be used to support private communications. RSA can be used to generate digital signatures, encrypt messages, and provide key management for DES (Data Encryption Standard), RC2 (Rivest Cipher 2), RC4 (Rivest Cipher 4), and other secret key algorithms. Two secret key encryption systems that are implemented in mass-market software. These systems are proprietary and are marketed by RSA Data Security, Inc. RC2 and RC4 can be used with various key lengths, such as 40 bits or 56 bits.
RPC (remote-procedure call)	The technological foundation of client-server computing. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the clients. See also client-server computing. A technology in which a program invokes services across a network by making modified procedure calls. The NFS protocol uses a specific type of RPC. A programming mechanism for clients to call routines over the network. RPC was originated by SUN Microsystems and is defined by RFC 1057. RPCS are often used to create distributed applications.
Seal	A checksum, which may be cryptographic, computed over some data to provide integrity for that data. A cryptographic checkvalue that supports integrity but does not protect against forgery by the recipient (i.e., it does not support non-repudiation). When a seal is associated with a data element, that data element is 'sealed'.

Term	Definition
Secret Key	In a symmetric cryptographic algorithm the key shared between two entities. In a symmetric encipherment algorithm the key shared between two entities. The key that two parties share and keep secret for secret key cryptography. Given secret key algorithms of equal strength, the approximate difficulty of decrypting encrypted messages by brute force search can be measured by the number of possible keys. For example, a key length of 56 bits is over 65,000 times stronger or more resistant to attack than a key length of 40 bits.
Secret Key Cryptography	Cryptography based on a single key (or symmetric cryptography). It uses the same secret key for encryption and decryption. Messages are encrypted using a secret key and a secret key cryptographic algorithm, such as Skipjack, DES (Data Encryption Standard), RC2, or RC4.
Security Certificate	A set of security relevant data which is protected by integrity and data origin authentication from an issuing security authority. It and includes an indication of a time period of validity. Note: All certificates are deemed to be security certificates (see the relevant definitions in 7498-2). The term "security certificate" is adopted in order to avoid terminology conflicts with [X.509 | ISO 9594-8] (i.e. the directory authentication standard).
Shoulder surfing	Stealing passwords or PINs by looking over someone's shoulder.
SLIP (Serial Line IP)	Serial Line Internet Protocol. A standard for point-to-point serial connections using TCP / IP. PPP is the TCP / IP protocol that enables dial-up networking from a computer equipped with a modem. RFC 105s describes slip. A framing protocol used to send IP across a serial line. SLIP is popular when sending IP over dialup phone lines. See PPP.
Spoofing	Using various techniques to subvert IP-based access control by masquerading as another system by using their IP address.
SSL (Secure Sockets Layer)	A security protocol developed by the Netscape Communications Corporation to encrypt sensitive data and verify server authenticity.
TCP / IP (Transmission Control Protocol / Internet Protocol)	The suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of worldwide Internetworks. Today, millions of users are connected to the Internet through software that uses the TCP / IP protocol suite.
Telnet	Protocol used for (possibly remote) login to a computer host
Transparent Proxy	A transparent proxy provides the ability to use an application process running on a firewall without explicitly requiring the client to specify that proxy. In other words, the client perceives that it is still speaking to the router gateway. This makes it considerably easier to install a firewall without having to reconfigure every client in a TCP / IP environment.
Trusted Network	Users on this network are, by default, deemed to be trustworthy. Users may be physically on a common network, or linked together via a virtual private network (VPN).

Term	Definition
UDP	(User Datagram Protocol) The TCP / IP standard protocol that allows an application program on one host to send a Datagram to an application program on another. UDP uses IP to deliver datagrams but UDP includes a protocol port number, allowing the sender to distinguish among application programs on a given remote host. Unbind Protocol operation used to release an association between two application entities. The TCP / IP standard protocol that allows an application program on one machine to send a Datagram to an application program on another. UDP uses the Internet Protocol (IP) to deliver datagrams. Conceptually, the important difference between UDP datagrams and IP datagrams is that UDP includes a protocol port number, allowing the sender to distinguish among multiple application programs on a given remote machine. In practice, UDP also includes an optional checksum over the data being sent. A connectionless transport-layer protocol belonging to the Internet protocol family. A connectionless transport layer protocol belonging to the Internet protocol family. UDP adds reliability and mutliplexing to IP datagrams.
Untrusted Network	These are outside networks of various kinds, among the many thousands of networks connected to the Internet, or even untrusted networks that may be part of other departments or divisions within an organization
Virtual Private Network	By using encryption, a private network is created over a public network, i.e.(the Internet), where exclusive client and host communications can occur. A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component.
X.509 certificate	A small file containing, the subject's name, name of authority that signed certificate, subject's public key, owner's public key, issuer's signature, certificate authority's digital signature from which certificate derives its authenticity, validity period, and serial number.

Appendix A

Information Security Core Technology Status

Appendix B

System Technology Risk Matrix

Appendix C

SFA Due Diligence Checklist

Appendix D

External Connectivity Self Audit Evaluation Criteria

Appendix E

Minimum Security Baseline